IN THE CLAIMS

1-33. (cancelled)

34. (currently amended) An information processing device operable within a node of a hierarchical network of nodes having a hierarchical tree structure, said information processing device comprising:

storage operable to store one or more node keys, each node key being unique to one node of the network, and a leaf key, the leaf key being unique to the information processing device and unique in relation to a leaf key held by any other node within the hierarchical network of nodes; and

an encryption processor operable to ~~perform encryption processing to~~:

calculate a decryption key by decrypting a key block using at least one of the one or more node keys stored in the storage or the leaf key stored in the storage,

encrypt the decryption key using the leaf key of the information processing device, ~~and~~

store the encrypted decryption key in at least one of the storage or on a recording medium together with a generation number, the generation number representing renewal information for the decryption key, and

use the generation number to determine whether it is necessary to decrypt a key block corresponding to the generation number to obtain the decryption key.

35. (cancelled)

36. (previously presented) The information processing device as claimed in claim 34, wherein

the key block includes an encrypted renewal node key, and

the encryption processor is further operable to decrypt the encrypted renewal node key to obtain the renewal node key using at least one of the node key stored in the storage or a leaf key belonging to a lower layer of the hierarchical network, and

stored in the storage, and to calculate the decryption key using the obtained renewal node key.

37. (cancelled)

38. (currently amended) The information processing device as claimed in claim 34, wherein the encryption processor is operable to store the decryption key encrypted using the ~~first~~ leaf key ~~unique to the information processing device~~, the encrypted decryption key being stored together with identification information, the identification information being unique to the information processing device.

39. (currently amended) The information processing device as claimed in claim 34, wherein the encryption processor is operable to store the decryption key encrypted using the ~~first~~ leaf key ~~unique to the information processing device~~, the encrypted decryption key being stored together with identification information, the identification information identifying data decrypted using the decryption key.

40. (previously presented) The information processing device as claimed in claim 34, wherein the decryption key is usable to decrypt encrypted content data in the information processing device.

41. (previously presented) The information processing device as claimed in claim 34, wherein the decryption key is stored on the recording medium and the decryption key is assigned to the recording medium, the decryption key being usable to decrypt encrypted data stored on the recording medium.

42. (previously presented) The information processing device as claimed in claim 34, wherein the decryption key is held in common by a plurality of the information processing devices, the decryption key being a master key usable to decrypt encrypted data in each of the plurality of information processing devices.

43. (currently amended) An information processing device

operable within a node of a hierarchical network of nodes having a hierarchical tree structure, said information processing device comprising:

storage operable to store a node key and a leaf key, the leaf key being unique to the information processing device and unique in relation to a leaf key held by any other node within the hierarchical network of nodes, and the node key being unique to each node of the hierarchical network of nodes; and

an encryption processor operable to ~~perform encryption processing to~~:

decrypt a key block using at least one of the node key stored in the storage or the leaf key stored in the storage to calculate a decryption key, ~~and to~~

store the decryption key in the storage together with a generation number representing renewal information for the decryption key,

determine whether the decryption key having the generation number is stored in the storage, and if so,

retrieve the decryption key from the storage for use in decrypting encrypted data without having to decrypt the key block.

44. (currently amended) An information processing device operable within a node of a hierarchical network of nodes having a hierarchical tree structure, each said information processing device comprising:

storage operable to store a node key and a leaf key, the leaf key being unique to the information processing device and unique in relation to a leaf key held by any other node within the hierarchical network of nodes, and the node key being unique to each node of the hierarchical network of nodes; and

an encryption processor operable to perform encryption processing to:

decrypt a key block using at least one of the node key

stored in the storage or the leaf key stored in the storage to calculate a decryption key, and to

store the decryption key in the storage together with identification information, the identification information being usable to identify data decrypted using the decryption key,

determine whether the decryption key corresponding to the identification information is stored in the storage, and if so,

retrieve the decryption key from the storage for use in decrypting encrypted data without having to decrypt the key block.

45. (currently amended) An information processing device operable within a node of a hierarchical network of nodes having a hierarchical tree structure, said information processing device comprising:

storage operable to store a node key and a leaf key, the leaf key being unique to the information processing device and unique in relation to a leaf key held by any other node within the hierarchical network of nodes, and the node key being unique to each node of a hierarchical network of nodes having a hierarchical tree structure; and

a decryption processor operable ~~to perform decryption processing~~ to:

use a generation number representing renewal information for a decryption key stored on at least one of the information processing device or the recording medium to detect whether an encrypted version of the decryption key for decrypting encrypted data is stored on at least one of the information processing device or a recording medium, and when the encrypted decryption key is detected, to calculate the decryption key by decrypting the encrypted decryption key, and

when the encrypted decryption key is not detected, to calculate the decryption key by decrypting a key block using at least one of the one or more node keys stored in the storage or

the leaf key stored in the storage.

46. (previously presented) The information processing device as claimed in claim 45, wherein, when the decryption key is not detected, the decryption processor is further operable to encrypt the calculated decryption key and to store the encrypted decryption key on at least one of the recording medium or the memory.

47. (previously presented) The information processing device as claimed in claim 45, wherein the decryption processor is further operable to decrypt the encrypted decryption key using at least one key unique to the information processing device when the encrypted decryption key is detected.

48. (currently amended) An information processing method, comprising:

storing one or more node keys and a leaf key in an information processing device of one node of a hierarchical network of nodes having a hierarchical tree structure, each node key being unique to one node of the network, the leaf key being unique to the information processing device such that each leaf key of each information processing device of the network is unique with respect to a leaf key of any other information processing device of the network;

decrypting a key block using at least one of the stored node key and the stored leaf key;

calculating a decryption key usable to decrypt encrypted data stored on at least one of the information processing device or on a recording medium;

encrypting the decryption key using the leaf key of the information processing device; and

storing the encrypted decryption key on at least one of the information processing device or on the recording medium <u>together with a generation number representing renewal information for the decryption key;</u>

using the stored generation number to determine whether the encrypted decryption key is stored on the at least one of the information processing device or on the recording medium; and

when it is determined that the encrypted decryption key is stored on the at least one of the information processing device or on the recording medium, using the leaf key to decrypt the encrypted decryption key to obtain the decryption key and using the decryption key to decrypt the encrypted data without having to decrypt the key block.

49. (cancelled)

50. (previously presented) The information processing method as claimed in claim 48, wherein the key block includes a renewal node key, the renewal node key being encrypted using at least one of the stored node key for the node or a leaf key belonging to a lower layer of the hierarchical network, and the decryption key is encrypted using the renewal node key, wherein the step of decrypting the key block includes decrypting the renewal node key using at least one of the stored node key and the stored leaf key, and the calculating step includes using the decrypted renewal node key to calculate the decryption key.

51. (previously presented) The information processing method as claimed in claim 48, wherein the storing step includes storing the decryption key encrypted using the leaf key, the encrypted decryption key being stored together with a generation number, the generation number representing renewal information for the decryption key.

52. (previously presented) The information processing method as claimed in claim 48, wherein the storing step includes storing the decryption key encrypted using the leaf key, the encrypted decryption key being stored together with identification information, the identification information being unique to the information processing device.

53. (previously presented) The information processing

method as claimed in claim 48, wherein the storing step includes storing the decryption key encrypted using the leaf key, the encrypted decryption key being stored together with identification information, the identification information identifying data decrypted using the decryption key.

54. (previously presented) The information processing method as claimed in claim 48, further comprising using the decryption key to decrypt encrypted content data in the information processing device.

55. (previously presented) The information processing method as claimed in claim 48, wherein the decryption key is assigned to the recording medium and is stored on the recording medium, further comprising using the decryption key to decrypt encrypted data stored on the recording medium.

56. (previously presented) The information processing method as claimed in claim 48, wherein the decryption key is held in common by a plurality of the information processing devices, the method further comprising using the decryption key as a master key to decrypt encrypted data in each of a plurality of information processing devices in the network.

57. (currently amended) An information processing method, comprising:

storing a node key and a leaf key in an information processing device, the leaf key being unique to the information processing device and the node key being unique to each node of a hierarchical network of nodes having a hierarchical tree structure such that each leaf key of each information processing device of the network is unique with respect to a leaf key of any other information processing device of the network;

decrypting a key block using at least one of the stored node key or the stored leaf key;

calculating a decryption key used to decrypt encrypted data;

storing the calculated decryption key in the information

processing device together with a generation number, the generation number representing renewal information for the decryption key;

using the stored generation number to determine whether the decryption key is stored in the information processing device; and

when it is determined that the decryption key is stored in the information processing device, using the decryption key to decrypt the encrypted data without having to decrypt the key block.

58. (currently amended) An information processing method, comprising:

storing a node key and a leaf key in an information processing device, the leaf key being unique to the information processing device and the node key being unique to each node of a hierarchical network of nodes having a hierarchical tree structure such that each leaf key of each information processing device of the network is unique with respect to a leaf key of any other information processing device of the network;

decrypting a key block using at least one of the stored node key or the stored leaf key;

calculating a decryption key used to decrypt encrypted data;

storing the calculated decryption key in the information processing device together with identification information, the identification information being usable to identify data decrypted using the decryption key;

using the stored identification information to determine whether the decryption key is stored in the information processing device; and

when it is determined that the decryption key is stored in the information processing device, using the decryption key to decrypt the encrypted data without having to decrypt the key block.

59. (currently amended) An information processing method, comprising:

storing a node key and a leaf key in an information processing device, the leaf key being unique to the information processing device and the node key being unique to each node of a hierarchical network of nodes having a hierarchical tree structure such that each leaf key of each information processing device of the network is unique with respect to a leaf key of any other information processing device of the network; ~~and~~

obtaining a generation number, stored on at least one of the information processing device or on a recording medium, the generation number being representative of renewal information for a decryption key, using the generation number to determine~~determining~~ whether an encrypted decryption key for decrypting encrypted data is stored on the at least one of the information processing device or on a recording medium,

when the encrypted decryption key is detected, decrypting the encrypted decryption key without having to decrypt a key block, and

when the encrypted decryption key is not detected, decrypting a key block using at least one of the one or more stored node keys or the stored leaf key and using the decrypted key block to calculate the decryption key.

60. (previously presented) The information processing method as claimed in claim 59, further comprising using at least one of the one or more stored node keys or the leaf key to encrypt the calculated decryption key and storing the encrypted decryption key on at least one of the recording medium or on the information processing device.

61. (previously presented) The information processing method as claimed in claim 59, wherein, when the encrypted decryption key is detected, the encrypted decryption key is decrypted using at least one key unique to the information processing device.

62. (currently amended) A recording medium having a computer program recorded thereon for performing a method, the method comprising:

storing one or more node keys and a leaf key in an information processing device of one node of a hierarchical network of nodes having a hierarchical tree structure, each node key being unique to one node of the network, the leaf key being unique to the information processing device such that each leaf key of each information processing device of the network is unique with respect to a leaf key of any other information processing device of the network;

decrypting a key block using at least one of the node key stored in the storage or the leaf key stored in the storage;

calculating a decryption key usable to decrypt encrypted data stored on at least one of the information processing device or on a recording medium;

encrypting the decryption key using the leaf key of the information processing device; and

storing the encrypted decryption key on at least one of the information processing device or on a recording medium together with a generation number representing renewal information for the decryption key;

using the stored generation number to determine whether the encrypted decryption key is stored on the at least one of the information processing device or on the recording medium; and

when it is determined that the encrypted decryption key is stored on the at least one of the information processing system or on the recording medium, using the leaf key to decrypt the encrypted decryption key to obtain the decryption key and using the decryption key to decrypt the encrypted data without having to decrypt the key block.

63. (currently amended) A recording medium having a computer program recorded thereon for performing a method, the

method comprising:

storing a node key and a leaf key in an information processing device, the leaf key being unique to the information processing device and the node key being unique to each node of a hierarchical network having a hierarchical tree structure, each node including at least one such information processing device such that each leaf key of each information processing device of the network is unique with respect to a leaf key of any other information processing device of the network;

decrypting a key block using at least one of the node key ~~stored in the storage~~ or the leaf key stored in the ~~storage~~information processing device;

calculating a decryption key used to decrypt encrypted data;

storing the calculated decryption key in a memory of the information processing device together with a generation number, representing renewal information for the decryption key;

using the stored generation number to determine whether the decryption key is stored in the memory of the information processing device; and

when it is determined that the encrypted decryption key is stored in the information processing device, using the leaf key to decrypt the encrypted decryption key to obtain the decryption key and using the decryption key to decrypt the encrypted data without having to decrypt the key block.

64. (currently amended) A recording medium having a computer program recorded thereon for performing a method, the method comprising:

storing a node key and a leaf key in an information processing device, the leaf key being unique to the information processing device and the node key being unique to each node of a hierarchical network of nodes having a hierarchical tree structure, each node including at least one such information processing device such that each leaf key of each information

processing device of the network is unique with respect to a leaf key of any other information processing device of the network; ~~and~~

obtaining a generation number, stored on at least one of the information processing device or on a recording medium, the generation number being representative of renewal information for a decryption key;

using the generation number to detect ~~determining~~ whether an encrypted decryption key for decrypting encrypted data is stored on at least one of the information processing device or on a storage medium~~,~~;

when the encrypted decryption key is detected, using the at least one of the node key or the leaf key of the information processing device to decrypt the encrypted decryption key to obtain the decryption key without having to decrypt the key block; and

when the encrypted decryption key is not detected, decrypting a key block using at least one of the one or more stored node keys or the stored leaf key and using the decrypted key block to calculate the decryption key.

65. (previously presented) A recording medium as claimed in claim 64, wherein the method further comprises using at least one of the one or more node keys or the leaf key to encrypt the calculated decryption key and storing the encrypted decryption key on at least one of the recording medium or on the information processing device.

66. (currently amended) A recording medium having encrypted information recorded thereon including at least one of audio information, video information or human language text information in encrypted form, the encrypted information being decryptable only by any one of a plurality of information processing devices using a decryption key, the recording medium having the decryption key recorded thereon in encrypted form,

the encrypted decryption key having been encrypted using a leaf key unique to one information processing device, the encrypted decryption key being stored as a key storage table together with identification information for the one information processing device, the identification information being usable to determine whether the decryption key corresponding to the encrypted data is stored on the at least one of the information processing system or on the recording medium, and if so, the decryption key being usable to decrypt the encrypted data.

67. (previously presented) The recording medium as claimed in claim 66, wherein the recording medium is removably insertable into any information processing device of the plurality of information processing devices through an opening in an exterior housing of such information processing device, and is recordable to store the encrypted decryption key when the recording medium is inserted into the one information processing device.

68. (previously presented) The recording medium as claimed in claim 62, wherein the method further comprises accessing the stored encrypted decryption key, recovering the decryption key by decrypting the encrypted decryption key using the leaf key, and decrypting content information stored on at least one of the recording medium or the storage using the recovered decryption key.

69. (previously presented) The recording medium as claimed in claim 67, wherein the decryption key includes a media key.

70. (previously presented) The information processing apparatus as claimed in claim 34, wherein the encryption processor is further operable to access the stored encrypted decryption key, recover the decryption key by decrypting the encrypted decryption key using the leaf key, and decrypt content information stored on at least one of the recording medium or the storage using the recovered decryption key.

71. (previously presented) The information processing apparatus as claimed in claim 70, wherein the decryption key includes a media key.

72. (previously presented) The information processing method as claimed in claim 48, further comprising accessing the stored encrypted decryption key, recover the decryption key by decrypting the encrypted decryption key using the leaf key, and decrypting content information stored on at least one of the recording medium or the storage using the recovered decryption key.

73. (previously presented) The information processing method as claimed in claim 72, wherein the decryption key includes a media key.